引用格式:孙恩昌, 董潇炫, 张卉, 等. 区块链赋能联邦学习:方法、挑战与展望[J]. 北京工业大学学报, 2025, 51(3): 337-349.
SUN E C, DONG X X, ZHANG H, et al. Blockchain enabled federated learning: approaches, challenges, and prospects [J]. Journal of Beijing University of Technology, 2025, 51(3): 337-349. (in Chinese)

区块链赋能联邦学习:方法、挑战与展望

孙恩昌[1,2], 董潇炫[1,2], 张 卉[1,2], 李梦思[1,2], 张冬英[3]
(1. 北京工业大学信息学部, 北京 100124; 2. 先进信息网络北京实验室, 北京 100124;
3. 北京工业大学网络与信息技术中心, 北京 100124)

摘 要: 针对区块链技术与联邦学习(federated learning, FL)结合后在安全、隐私等方面存在的问题,对区块链赋能FL中的相关方法进行综述与分析。首先,分别阐述了FL和区块链,并在此基础上总结了区块链赋能FL的前沿通用架构;其次,研究了目前安全、隐私、激励以及效率方法的进展,分析了各方法的优缺点;最后,指出了区块链赋能FL目前存在的问题,提出了解决方案,并进行了展望。

关键词: 联邦学习(federated learning, FL); 区块链; 数据安全; 数据隐私; 激励机制; 效率
中图分类号: TN 915 **文献标志码**: A **文章编号**: 0254 - 0037(2025)03 - 0337 - 13
doi: 10.11936/bjutxb2023060014

Blockchain Enabled Federated Learning: Approaches, Challenges, and Prospects

SUN Enchang[1,2], DONG Xiaoxuan[1,2], ZHANG Hui[1,2], LI Mengsi[1,2], ZHANG Dongying[3]
(1. Faulty of Informational Technology, Beijing University of Technology, Beijing 100124, China;
2. Beijing Laboratory of Advanced Information Networks, Beijing 100124, China;
3. Network and Information Technology Center, Beijing University of Technology, Beijing 100124, China)

Abstract: In response to security and privacy in the integration of blockchain technology with federated learning (FL), comprehensive review and analysis of the relevant methods for empowering FL with blockchain are provided. First, FL and blockchain were elucidated separately, and on the basis of this, the state-of-the-art general architectures for blockchain-enabled FL were summarized. Second, the progress in security, privacy, incentives, and efficiency methods was investigated, and the advantages and disadvantages of each method were analyzed. Finally, the current issues in blockchain enabled FL were identified, and potential solutions were proposed, along with future prospects.

Key words: federated learning (FL); blockchain; data security; data privacy; incentive mechanism; efficiency

---

收稿日期: 2023-06-08; 修回日期: 2023-09-09
基金项目: 国家自然科学基金资助项目(61671029); 北京市自然科学基金资助项目(L211002); 北京市教育委员会科技计划资助项目(KM202110005021)
作者简介: 孙恩昌(1977—), 男, 副教授, 主要从事无线通信与网络、区块链、联邦学习、深度学习方面的研究, E-mail: ecsun@bjut.edu.cn

近年来,随着计算能力、算法和数据量的不断提高,人工智能领域的机器学习方法迎来了飞速发展,从人脸识别到精确预测,已广泛应用于日常生活中[1-4]。然而,机器学习是一种需要大量数据支持的训练方式,因此,数据隐私和保护成为备受关注的问题[5],从而出现联邦学习(federated learning,FL)技术。FL 允许用户协作训练一个共享的学习模型,但是不共享自己的原始数据,只上传训练后的模型参数。与传统的机器学习相比,FL 可以保护客户端的数据,防止本地数据隐私的泄露,因此,目前 FL 得到了广泛应用。

尽管 FL 本身在保护数据隐私方面表现优异,但是在安全、激励等方面仍然存在一些隐患。首先,模型的聚合完全依赖于中央服务器,中央服务器的不稳定会造成单点故障(single point of failure,SPoF)。其次,客户需要完全信任参与者,但这在现实中往往难以实现,恶意参与者的存在可能对整个训练过程造成破坏,这就需要有效的监管机制以及奖惩机制防止恶意参与者进行恶意更新或者破坏。除此之外,进行模型训练需要消耗大量计算资源和存储资源,使得通过建立合理的激励机制给予参与者补偿极为重要。

区块链赋能 FL 可以有效解决上述的安全和激励方面的问题,作为一种去中心化的账本技术,区块链所具有的不可篡改性、历史可追溯性等特点可以确保模型更新在分散存储的同时具有可审计性。区块链中的各区块之间通过哈希值按照时间顺序进行连接,使其可以准确地记录历史数据。同时,通过工作量证明(proof of work, PoW)等共识机制的实行,保证了区块链全网记录的一致性和不可变性。区块链赋能 FL 使得 FL 可以通过分布式的方式进行模型训练,从而在一定程度上避免了中央服务器带来的安全问题。除此之外,激励制度的合理运用可以有效调动参与者的积极性,但由于区块链的加入,增加了一定的时间成本和计算开销,在一定程度上降低了系统效率。

本文针对区块链赋能 FL 技术,分析了相关的研究文献。首先,对 FL 和区块链 2 个技术进行了阐述;其次,从系统安全、信息隐私以及激励 3 个方面分析了区块链赋能 FL 的优势,并总结了区块链赋能 FL 的通用架构;然后,全面研究了该架构目前在安全、隐私、激励以及效率方面的最新进展,深入分析了各方法的优缺点;最后,指出了区块链赋能 FL 目前存在的挑战,并展望了未来的解决方法。

1 FL

1.1 概念

FL[6]在 2016 年由谷歌提出,是一种集中式的训练机制,这种机制通过共享参数而不是数据本身的方式保证用户隐私。

FL 的工作过程分为训练和聚合 2 个阶段(见图 1),将模型训练者(FL 参与者)集合称 W,在一次 FL 训练轮次 t 中,FL 将初始模型更新下发给 W,然后每一个参与训练的设备 $w(w \in W)$ 基于自身本地的数据集对这个初始模型进行训练。具体来说,就是在每一轮训练回合中,每一个设备训练一个本地模型,用 l_w^t 表示,并通过最小化损失函数 $F(l_w^t)$ 计算得到更新 l_w^{t+1}。其中最小化损失函数可以是不同的[7]。

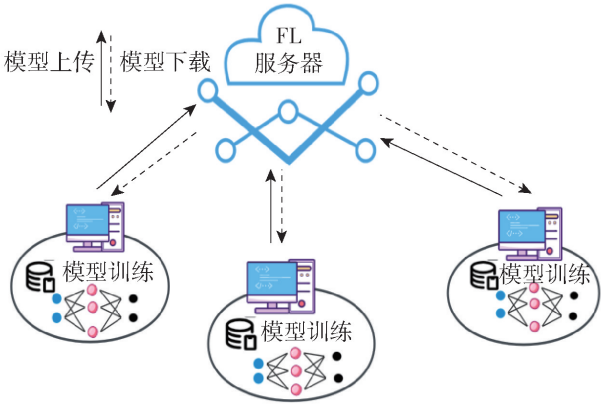

图 1 传统 FL 工作过程

Fig. 1 Work process of classical FL

之后,w 将更新 l_w^{t+1} 作为本地模型上传至中央服务器进行模型聚合,生成的全局模型供用户下载,公式为

$$G_{t+1} = G_t + \frac{1}{m} l_w^{t+1}$$

式中:G_t 为第 t 个轮次的全局模型;G_{t+1} 为新生成的第 $t+1$ 个轮次的全局模型;m 为参与者数量。

FL 通过联邦平均算法(federated averaging algorithm, FedAvg)及其改进算法完成模型聚合工作。FedAvg 算法经过泛化及再参数化后被命名为 FedProx[8],用于处理系统的异质性。除此之外,对聚合算法的改进还有联邦匹配平均算法(federated matched averaging algorithm, FedMa)以及联邦优化等,它们可以用来解决 FL 聚合过程中的不同类型的问题[9]。

基于数据集的分布属性,FL 又可以被分为 3 种

类型：水平联邦学习（horizontal federated learning，HFL）、垂直联邦学习（vertical federed learning，VFL）以及联邦迁移学习（federated transfer learning，FTL）[10]。

HFL，又称作基于样本的 FL，是在数据集共享相同的特征空间但样本不相同的情况下引入的，即取出具有相同业务需求的用户数据以扩大训练的样本空间。在 2016 年，谷歌提出了一种水平 FL 方法[6]。HFL 通常假设有安全的参与者，即通常情况下只有中央服务器可以造成隐私泄露或者破坏。

VFL 又称作是基于特征的 FL，适用于 2 个数据集共享相同的样本空间但特征空间不同的情况，即取出具有不同业务需求的用户数据进行联合训练以增强用户训练模型的效果。VFL 中通常假设用户端可能造成隐私泄露或者破坏。

FTL 结合了迁移学习技术[11]，适用于数据集样本空间和特征空间都不同的情况，不对数据集进行切分，应用范围更加广泛。FTL 利用迁移学习技术可以克服数据集间用户和用户业务需求相似度少引起的训练数据不足的问题。在 FTL 中通常假设参与的每一方都诚实完成训练任务，但是尝试推测其他参与方的数据集。

1.2　FL 面临的问题

1）SPoF。传统的 FL 系统严重依赖中央服务器，而中央服务器可能存在各种安全隐患：①中央服务器不稳定会造成系统全面崩溃；②中央服务器被破坏形成假的全局模型，并伴随隐私泄露风险；③系统资源的巨大消耗。FL 架构很容易因 SPoF[12-13] 导致中央服务器崩溃，无法完成 FL 训练。

2）成员推理攻击。该攻击是一种针对模型数据、用户数据的隐私攻击技术[14]，目的是判断数据是否源自 FL 参与者的训练集，如果属于训练集，则为成员，否则为非成员，其本质上是对未知来源的数据进行二次分类，给出成员数据或者非成员数据的判定。成员推理攻击可以使攻击者获得训练集数据共有的特征，是很多模型隐私攻击的基础，模型窃取、数据重建等隐私攻击都建立在成员推理攻击的基础上，因此，成员推理攻击可以用于评估模型的隐私泄露程度。

3）中毒攻击。该攻击可分为数据中毒和模型中毒。数据中毒一方面可以改变模型的训练数据，从而使得 FL 参与者传播虚假模型，另一方面还可以改变数据的标签，这属于预定义的有毒模型更新，使得系统整体训练的模型精度下降，因此，数据中毒攻击最终可导致模型中毒。除此之外，FL 系统中还存在随机和逆向模型投毒攻击，前者的模型更新由任意的梯度更新形成，后者使模型训练朝着训练目标的反方向更新[15-17]。

2　区块链

2.1　概念

从网络层面讲，作为比特币[18]的底层技术，区块链以去中心化账本技术而闻名，运行在一个对等网络（peer to peer，P2P）上，网络中的节点地位相等，不存在中央服务器，节点并不受任意实体的控制[19]，而是共同维护一个公共可信且可共享的账本，存储完整的事务日志[20]，保持无法篡改的交易记录，这就避免了中心化造成的 SPoF 的问题。此外，区块链还是一个拜占庭容错的分布式系统[21]，这使得即使在一些节点发生故障的情况下整个网络仍然能够继续运行并提供服务。区块链如今已经被运用到了物联网[17]、医疗管理[22]等多个领域。

区块链可以分为 3 种类型：公有链、联盟链以及私有链。公有链是指完全开放的区块链网络，任意节点都可以选择加入或者退出。网络中不存在支配性的节点，任意节点都可以参与验证事务，参与共识过程，最常见的有以太坊[23]和比特币。但是，公有链的交易速度慢，吞吐量低。与之不同的是联盟区块链只面向一定的组织开放，只有组织中的成员才具有读写权限，但是节点的权利并不完全对等，一些特殊节点被赋予验证新区块的特权，其他节点也可以进行验证，但是要达成共识才能实施。相对公有链而言，联盟链在交易速度以及吞吐量上都有一定提升，典型代表有 Hyperledger Fabric[24]。私有链指的是面向单个组织开放的区块链网络，它的效率更高，易于实施，消耗的能量更少。

2.2　数据结构

区块链是一种按照时间顺序排列区块的链式数据结构，区块间通过哈希指针进行链接，使用密码保证区块内容不被篡改。每一个区块都分为区块头和区块体 2 个部分，其中在区块体中存储事务，在区块头中存储时间戳、随机值、默克尔根以及前一个区块的哈希值等内容，比如，在比特币中，区块链节点通过寻找合适的随机值的方式达到 PoW 共识。默克

尔树是一种二叉树结构,其中默克尔根是它的根节点,其叶节点是区块体中交易的哈希值,中间节点是将叶子结点哈希值拼在一起后计算得到的哈希值,如果有任意一个节点中的交易被篡改就会从下到上使默克尔根发生改变,因而可以作为验证交易正确性的方式。

2.3 共识算法

共识算法是区块链中最关键、最核心的技术,主要解决了谁来记账和如何保证全网记录一致这 2 个问题,可以保证区块链在有一定恶意节点存在的情况下仍能正常运行。

目前,常见的共识算法可以分为 2 类:主要应用于公有链的中奖类共识算法和主要应用于联盟链的投票类共识算法。中奖类共识算法的代表是比特币使用的 PoW 共识算法,除此之外常见的还有能力证明(proof of capacity, PoC)共识算法[25]、权益证明(proof of stake, PoS)共识算法[26]等。投票类共识算法比较典型的是拜占庭容错(practical Byzantine fault tolerance, PBFT)共识算法[27]。这类算法常应用在节点数量较多的区块链网络中,但是由于需要进行多轮通信和广播,增加了通信开销的同时降低了系统效率。

2.4 智能合约

智能合约[28]是部署在区块链上的一种数字协议,本质上是写入区块链系统的脚本代码。通过预定义的方式,当满足协议中的某一个条件时触发协议自动执行预先编辑好的代码而不需人工干预。智能合约使区块链从单纯的分布式存储架构变成了分布式计算架构,极大拓宽了应用场景。

3 区块链赋能 FL 基本框架

首先,使用去中心化的区块链可以代替中央服务器,通过全局共享的不可更改的账本进行模型聚合并下发,不仅降低了 SPoF 风险,同时也减轻了中央服务器进行全局聚合的负担,尤其是在系统内的设备较多的时候。其次,将更新存储到区块链中供客户端之间进行信息共享,既保证了透明性和不可篡改性,同时也可以有效防御外界攻击。最后,区块链的激励制度可以有效吸引参与者加入模型训练。

区块链赋能 FL 的架构主要包括 5 个部分:1) FL 参与者;2) 智能合约;3) 共识算法;4) 区块链节点;5) 区块链网络。

下面对区块链赋能 FL 的工作流程进行概括,如图 2 所示。工作流程共有 5 个步骤:

1) 当网络中发布特定的训练任务之后,对本次任务的 FL 参与者以及区块链节点进行初始化,同时为 FL 参与者下发初始训练模型。

2) 本地模型训练 FL 参与者下载全局模型,并使用本地数据集对本轮的全局模型进行训练以得到本地模型更新,并通过创建事务的方式上传给区块链节点。

3) 区块链节点接收到模型后按照特定的数据结构(比如默克尔树)存储它们,并且生成独特的时间戳、随机数以及唯一的哈希值,防止该区块被复制或者篡改。

4) 所有区块链节点同时执行共识算法,对新生成的块进行验证,在所有区块链节点达成共识后,新生成的区块被广播给网络中所有区块链节点。

5) 当共识结束后,块被添加到区块链网络,同时所有区块链节点将该区块添加到本地链。FL 的所有参与者都可以对区块内容申请下载,直到全局模型的精度达到任务需求者的要求之后训练任务完成,否则将不断重复步骤 2) ~5)。

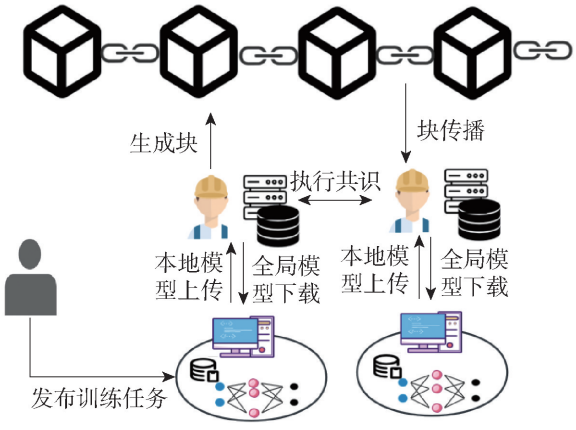

图 2 区块链赋能 FL 基本框架

Fig. 2 Basic framework of blockchain enabled FL

传统 FL 和区块链赋能 FL 的比较如表 1 所示。可以看出,通过融合区块链,FL 可以允许更多设备加入,区块链分散的网络拓扑结构可以使系统获得更好的扩展性。除此之外,模型通过不可更改的区块的形式进行存储也提高了训练模型的安全性[29]。区块链赋能 FL 的架构由于其安全性以及去中心化的特点体现出来巨大的发展潜力,但是,该框架仍然存在引入区块链造成的通信开销、通信延迟以及效率降低等问题。

表 1　传统 FL 与区块链赋能 FL 的比较

Table 1　Comparison between classical FL and blockchain enabled FL

FL 类型	优点	缺点
传统 FL	本地训练而不上传数据本身 保护数据隐私 节省网络、带宽资源	仍然存在安全问题(例如数据攻击、SPoF) 远程设备与服务器的通信延迟高 模型聚合不透明,缺乏激励机制
区块链赋能 FL	不需要中央服务器避免 SPoF 在设备和服务器之间建立信任 提高 FL 的可扩展性 通过激励机制提高参与度	区块链挖掘引起时间延迟 共识过程增加计算与通信开销 开放更新共享可能带来隐私风险 训练数据与区块链存储可能存在冲突

4　区块链赋能 FL 研究现状

4.1　安全和隐私

在 FL 过程中模型存储和聚合都由中央服务器完成,因而中央服务器的稳定性和安全性直接影响整个系统的性能,具有去中心化结构的区块链成为一个理想的解决方法[30-33]。其中文献[30,32-33]都把模型聚合任务交给了训练节点,不同的是在文献[33]中,区块链仅存储本地模型,在每一轮次的全部本地模型上传到区块链之后,各训练节点将模型下载后自行在本地进行聚合并开启下一轮的训练。在文献[30]提出的 ST-BFL 架构中,引入了星际文件系统(interplanetary file system, IPFS)存储模型。ST-BFL 采用同态加密、FL 聚合器、FL 验证器和智能合约,实现了输入隐私、输出隐私、输出验证和流量治理等各种结构化透明组件,全局模型通过智能合约选择聚合节点和一定数量的验证节点进行聚合,验证后上传至 IPFS,同传统方案相比克服了集中式聚合服务器可能由于攻击或物理损坏而发生故障的问题,但是却产生了更多的通信花销。在文献[32]中,只将全局模型存储于区块链上,训练节点同时担当区块链网络的节点,并且每个节点都会进行模型聚合,最终通过共识选择出打包区块的节点,避免了中央服务器由于故障或遭受攻击带来的安全隐患。除此之外,对于文献[30]中存在的通信开销问题,文献[32]通过优化通信次数的方式进行合理的资源分配,达到了消耗少的目标。文献[31]将模型聚合任务交给区块链,文中提出的 Chain FL 采取了分片的方式,一个服务分片中至少分配一个区块链节点负责。每个训练者在获得本地模型后就将本地模型上传至区块链节点,通过在线的方法并行聚合和模型更新,同时下载最新的全局模型进行下一轮训练,利用区块链的安全性实现了模型的安全聚合和存储,但是最后模型的精度相较于深度学习稍差。

在 FL 训练过程中可能存在恶意设备发起中毒攻击以及成员推理攻击,从而影响模型的质量[34-38],文献[34-36]通过验证生成的模型减少了可能存在的中毒攻击。文献[34]对本地模型进行加密之后,为其生成模糊哈希值,区块链可以通过模糊哈希值检测出模型的异常和变化,进而剔除被篡改过的模型达到抵抗中毒攻击的目的。除此之外,还通过通信协议(time-triggered protocol, TTP)使用区块链和智能合约增加了额外的安全层,该架构实现了在参与节点较多时可以检测出所有的中毒模型且不损害 FL 过程的安全要求。文献[34,36]对生成模型的质量进行验证,文献[34]对智能合约进行编写,添加评估函数和局部差分隐私技术。评估函数通过评估模型质量生成平均值,基于此剔除中毒模型,完成聚合工作,达到了抵抗中毒攻击的目的。同时,将局部差分隐私技术写入智能合约,该方式可以加强模型的隐私性以抵抗成员推理攻击,但是此框架仍存在聚合过程中设备的不公平使用,参与者过多时通信开销增大,从而影响 FL 的准确性等问题。针对文献[34]中存在的通信开销问题,文献[36]引入了梯度压缩,在保护数据的私密性的同时进一步降低通信成本,并且分别通过基于中值的测试和 Krum 算法测量局部和全局更新。这 2 种机制的结合实现了在每一轮中唯一地选择高质量的全局更新,同时能够及时发现模型被破坏。文献[37-38]都是通过提高模型的安全性抵抗中毒攻击和成员推理攻击的,在文献[37]中提出私有链邦联学习(private blockchain federated learning, PriChainFL)架构,引入了 IPFS 对本地模型进行存储,并将加密的哈希索引存储在区块链上,并通过区块链记录每个模型的训练事务实现了每代模型的记录存储以及可追溯,达到了防止成员推理攻击的目

的。此外,还使用指纹对交易进行加密,降低了模型中毒的风险,提高了模型的安全性。文献[38]则通过将本地差分隐私机制、区块链和 FL 相结合,授权区块链代替中央处理器,通过在模型训练结束后运用本地差分隐私机制加入随机噪声的方式加强数据的隐私保护、最小化来自恶意参与者发起的成员推理攻击,从而达到保护模型安全的目的。

综上所述,区块链赋能 FL 实现了对安全攻击的有效抵抗。在安全方面,攻击者可以通过对中央服务器发起攻击造成系统崩溃,尝试用设计好的伪造数据训练局部模型、替换全局模型,并在模型传输过程中通过修改参数值操纵训练输出以及通过模型推测其他节点信息等方式造成安全危机。本文对现有的安全方案做出总结(见表 2),现有的工作大多集中在检测本地模型以及增强模型保护。虽然结合了区块链之后,FL 的安全性得到了强有力的保障,但引入区块链带来更高的通信开销、更长的时间延迟等问题仍然需要进一步研究。目前,区块链赋能 FL 的安全方法在银行[32]、物联网[34]、5G 网络[35]、6G 网络[36]、车联网[39]等场景下得到了广泛应用,提高了 FL 抵御安全攻击的能力,保证了模型的安全,降低了 FL 的安全隐患。

表 2 区块链赋能 FL 安全方法

Table 2 Security methods of blockchain enabled FL

文献	区块链/共识	模型精度/%	主要贡献	不足
[30]	Ethereum/	98.59	保证可靠聚合,克服 SPoF 模型精确度未受损	通信花销高 模型聚合时间长
[31]	Ethereum/PoA	89.08	有效消除了 SPoF 采取分块形式,训练效率提高	模型精度略差 模型收敛速度慢
[32]	/PoW	80.00	克服了 SPoF 可识别懒惰客户端 模型及数据隐私性高	通信开销低 噪声添加影响模型精度
[33]	私有区块链/PoW	99.04	克服了 SPoF 通过激励机制提高了设备和样本的参与度 具有较高的扩展性	网络延迟略高
[34]	/PoW		保证了数据的安全性 抵抗中毒攻击 可检测出中毒模型 处理数据快、开销低	当验证事务较少或者边缘节点较少时,容易受到安全攻击
[35]	Ethereum/	99.21	通过自动验证模型更新抵御投毒攻击 通过差异隐私抵抗成员推理攻击	聚合过程中不公平使用设备 通信效率低 参与者过多时通信开销影响模型训练的准确性
[36]	/PBFT		抵抗中毒攻击 具有良好的效率和可扩展性 隐私性高 通信开销低	无法有效抵抗成员推理攻击 缺乏合理激励机制
[37]	私有区块链/	98.38	有效抵抗中毒攻击 存储成本低 系统鲁棒性好	时间成本高,不适用于时效性场景 存在训练设备信息泄露风险
[38]	Ethereum/	95.80	有效抵抗成员推理攻击 通过去中心化激励训练	噪声添加影响模型精度

4.2　隐私

针对 FL 进程中仍存在的数据泄露的情况，目前大多数工作都采取添加噪声或进行加密的手段来保护数据的隐私性[30,32,38,40-42]。

文献[32,38]采取了加入噪声的方式增强隐私性。在文献[38]中，当 FL 节点在完成本地训练生成模型之后，采取本地差分隐私机制为本地模型加入噪声，之后再进行上传聚合，噪声的添加增强了模型的隐私性，然而在一定程度上对模型的精度造成了影响。基于此，文献[32]在训练本地模型前让节点根据自身情况设置隐私预算并基于预算为模型添加噪声，隐私预算使得隐私性增强的同时对精度进行了平衡，但仍未完全解决问题。

文献[30,40-41]通过加密的方式增强隐私性。其中文献[30]通过同态加密的方式对训练好的模型使用公钥对应的密文进行加密，并上传至 IPFS，同时通过控制只有任务发布者可以查询存储在 IPFS 上的私钥及上下文的方式保护模型免受成员推理攻击，但却增加了开销。对于文献[30]中存在的开销问题，文献[40]提出了分散且保护隐私的聚合方案（decentralized and privacy-preserving aggregation scheme，DPPA），使用同态 Paillier 密码系统和数字签名批量验证算法，通过 Paillier 密码系统生成公私钥，并对本地模型和全局模型进行加密，数字签名批量算法将所有信息集合到一起后再进行加解密，使得攻击者无法获得单个节点的信息。该方案实现了保密性、不可篡改性以及不可否认性，同时有效降低了安全方面的计算开销，但仍会受到恶意节点破坏的影响。文献[41]针对文献[40]存在的恶意节点的问题，创建了一种新的函数加密方案，即非交互式指定解密函数加密（non-interactive designated decryptor function encryption，NDD-FE）方案。NDD-FE 避免了加密器和密钥生成器之间的多次交互，并实现了只有指定的解密器才能解密聚合的全局模型，从而避免了恶意节点造成的隐私泄露问题，同时，为了进一步降低通信开销，使用了深度梯度压缩算法。

除此之外，针对文献[32,38]中存在的噪声与精度之间的平衡问题，文献[42]结合了加密和噪声 2 种方式，在使用差分隐私添加噪声的同时引入了同态加密机制，将模型中的特征按照贡献进行排序，对高贡献的特征使用同态加密保证模型训练的精度，而对于低贡献部分则加入差分隐私噪声来保证隐私性，通过协调加密与加噪特征的比例实现了效率与精度方面的平衡。

综上所述，区块链赋能 FL 实现了对于数据和模型隐私的有效保护。在隐私方面，本文对基于区块链的 FL 隐私方案进行了总结（见表 3），现有的工作集中在添加噪声以及进行加密，从而增强数据和模型的隐私性，虽然在数据和模型保护方面取得了一定的进展，但是仍存在数据或模型进行加密或加噪声之后对全局模型精度造成影响、增加通信和计算开销的问题。区块链赋能 FL 的隐私方法在物联网[40,42]、数据分享[43]、医学图像检测[41]、车联网[44]等场景下得到广泛应用，有效提高了数据和模型隐私性，提高了抵御隐私攻击的能力，保护了数据安全。

表 3　区块链赋能 FL 隐私方法

Table 3　Privacy methods of blockchain enabled FL

文献	区块链/共识	模型精度/%	主要贡献	不足
[30]	Ethereum/	98.59	有效抵抗成员推理攻击 加密保护模型隐私	开销较高 聚合时间长
[38]	Ethereum/	95.80	有效抵抗成员推理攻击 保证了模型训练效率与精度	噪声的添加影响模型训练精度
[40]			有效抵抗成员推理攻击 训练效率高 有效降低安全方面的计算开销	容易受到恶意节点的破坏
[41]	/PoS	90.87	通信和计算成本低 保证数据和模型的安全性和隐私性	模型精确度略低
[42]		83.02	有效权衡效率和准确性 实现可信计算	增加通信开销 容易受到恶意模型需求者的破坏

4.3 激励

尽管 FL 实现了在保护用户隐私的同时完成协作学习,但是仍然面临着如何激励参与者贡献出数据和计算资源加入训练的问题,如果没有合理的激励机制,很可能出现没有足够的参与者的情况,从而影响训练。区块链可以完成经济透明的激励机制设计,从而成为解决该问题的一个极具吸引力的工具。现有的激励方案大致可以分为 2 种:1)基于声誉的激励机制[45-46];2)基于贡献的激励机制[38,40,47-52]。

基于节点声誉的激励方案通过评估节点行为、训练模型的质量对节点生成对应的声誉值,根据节点的声誉值选择节点并给予一定激励[45-46]。

在文献[45]中节点需要在规定时间内完成模型更新上传,之后使用本地数据集对其他节点提交的模型进行验证,评估节点声誉,对未提交模型、准确值低于阈值的节点给予负面评价,与此同时也会评估与自身模型的相似度以避免出现搭便车行为。智能合约根据声誉值进行激励,从而达到吸引节点参与并抵御恶意节点的效果。文献[46]提出了安全可靠的区块链 FL 框架(secure and trustworthy blockchain framework tailored to federated learning, SRB-FL)。该文献采取分片策略,引入了一种激励机制,利用主观多权逻辑设计了一个具有设备内部声誉和设备间声誉的声誉机制来提高 FL 器件的可靠性,其中,内部声誉由设备收集声誉之后进行分析得到,设备间声誉则由其他设备在观察目标设备后形成,将 2 种声誉进行加权结合后生成全局声誉再对节点进行激励。这种机制提高了声誉评价的客观性和公平性,能够有效地保证网络的可靠性、安全性和可扩展性。

基于贡献的激励方案通过评估模型的质量判断节点的贡献,并据此给出激励[47-52]。

文献[47]通过设计一种激励机制激励优秀的训练者和验证者,从而增加系统的安全性。该机制中存在 2 种类型的激励:一种是当模型被验证者验证为有效贡献时验证者支付的激励,另一种是区块链管理者对模型做出最佳贡献的验证者的激励,并据此选择谁将挖掘区块。2 种激励分别保证了模型的质量,防止了恶意设备频繁获得激励。文献[48]设计了一个在公共区块链网络上面向机制设计的 FL 协议,每轮训练结束后,下一轮参与者对上一轮训练的模型进行投票,并基于投票选出的优质模型进行下一轮训练,并在每一轮投票结束时将激励发给参与者。此协议引入了竞争机制来激励参与者,从而最大化参与者的激励,只有表现良好的参与者才能够得到激励,达到在不需要采取任何加密手段的情况下使参与者自觉遵守协议的目的,但系统仍存在恶意节点破坏的问题。针对这一不足,文献[49]提出的区块链驱动的安全和激励 FL(blockchain-empowered secure and incentive federated learning, BESIFL)框架开发了一种基于准确性的恶意节点检测机制,该机制能够在训练过程中检测到恶意节点对模型准确性的不利影响后立即识别并删除恶意节点,同时,对激励机制进行了改进,采用基于贡献的节点选择和基于令牌的节点激励机制,使提出的共识算法对模型精度达成共识,并通过精度评估训练参与者以及模型验证者的贡献,基于此进行激励以确保模型训练的安全性,同时鼓励可信节点参与 FL。不同于文献[48]中的竞争机制,文献[50]提出基于进化博弈论的动态激励模型,通过博弈论对用户在数据共享中的博弈过程进行了建模,找到满足用户策略稳定性的条件。根据数据的相似度和训练模型的质量评估数据提供者的贡献程度。对模型贡献更多的数据提供者将获得更多的信用币,从而吸引更多用户参与并训练高质量模型。文献[51-52]在区块链网络上使用智能合约实现激励,利用了区块链透明、独立和不可变的特性。在这种情况下,文献[51]使用基于以太坊区块链的智能合约来激励 FL 参与者,参与者的直观贡献与模型训练和激励过程相关联,从而促使更多训练者训练高质量模型。类似地,文献[52]提出利用区块链多维拍卖的 FL(federated learning-multi-auction using blockchain, FL-MAB)框架,引入了基于区块链的盈利方案,以及多维拍卖机制。框架中采用了一种在智能合约中运行的 FL 参与者选择机制,该机制在使用加密货币奖励参与者的同时根据参与者自身的资源选择参与者,包括参与者提供的计算和网络资源以及本地数据的质量。多维拍卖通过智能合约以可靠和可审计的方式实现,这允许 FL-MAB 通过计算 Shapley 值衡量每个客户的相对贡献,并进行相应的激励。此外,基于区块链的 FL 提供了不可抵赖性和完整性,并鼓励模型需求者使用加密货币作为激励。

综上所述,区块链赋能 FL 系统中的激励机制设计的目标是在训练中吸引更多的参与者和数据集,提高 FL 的鲁棒性。区块链的去中心化、可信度高等特点以及智能合约的存在为实现透明安全的激励提供了技术支持。模型更新由区块链或部

分节点进行验证和审计，而本地模型梯度收集和全局模型参数更新由区块链网络上的所有参与者监控，从而确保 FL 过程的公平性。本文对现有的 FL 中的激励方案进行了总结（见表 4），目前的工作在一定程度上提高了节点的参与度，进而保证了模型的训练精度。然而，恶意节点对系统的破坏仍然是较大的威胁，同时如何实现激励的绝对公平性仍需要进一步探讨。区块链赋能 FL 的激励方法目前在边缘移动网络[49]、物联网[40]、医疗系统[53]、边缘计算[54]等方面得到广泛应用，有效调动了参与训练的节点数量以及参与节点的积极性，提高了系统的稳定性。

表 4　区块链赋能 FL 激励方法

Table 4　Incentive methods of blockchain enabled FL

文献	区块链/共识	模型精度/%	主要贡献	不足
[46]	/PoW	95.58	模型精度高 有效抵抗搭便车攻击	对恶意节点容忍度略低
[47]	/PoW	98.01	具有可扩展性 可得出准确的声誉值	模型精度受到恶意 FL 节点的影响
[48]	/PoS	98.68	通信开销低 保证网络可靠性、安全性和可扩展性	未进行具体实现 模型损失不稳定
[49]		83.66	保证了工人自觉遵守协议 通过竞争最大化工人激励 模型精度高，收敛速度快	模型精度受到恶意 FL 节点的影响 未进行具体实现
[50]	/PoQ	94.48	有效抵抗恶意节点 模型收敛快、精度高	模型的隐私性略差
[51]	联盟链/	86.53	模型收敛速度快 保证激励的公平性 能够抵抗合谋攻击 通过博弈论实现了较高且稳定的用户参与度	用户参与度受成本的影响 不适用于中小型场景
[52]	联盟链/	96.02	具有可扩展性，性能稳定 具有有效的激励和惩罚机制	节点的贡献度量须进一步权衡

4.4　效率

区块链和 FL 都是需要大量资源消耗的技术，而且区块链的加入虽然消除了和中央服务器之间的通信引起的网络延迟，但是，同时也引入了与成块和共识相关的新的成本，要考虑到训练延迟、通信延迟以及共识延迟，因而，有许多工作致力于提高区块链赋能 FL 的工作效率[55-59]。

文献[55-56]采取了使用 2 种类型区块链的方式提高系统工作的整体效率。文献[55]设计了基于区块链的混合交易系统，采取联盟链和公有链 2 种区块链，通过公共链的智能合约设计了一个链下的支付通道，使得请求者可以在链下向节点支付激励，避免了链上操作造成的效率低下问题，同时采取异步全局聚合的方法，提高了模型收敛的速度。在文献[55]的基础上，文献[56]提出了用于 FL 的双层区块链集成框架，由本地模型更新链（local model update-chain，LMUC）和全局模型更新链（global model update chain，GMUC）这 2 种区块链构成。LMUC 负责按照时间顺序并采用防篡改的方式存储本地模型更新，同时引入终端直通（device-to-device communication，D2D）来帮助传输以减少共识和记录数据过程产生的延迟；GMUC 可以通过减少故障移动边缘节点和恶意本地设备引起的训练失败来安全地获得全局模型更新，同时 GMUC 中的移动边缘节点被组织成不同的碎片以提高区块链存储的效率。除此之外，该框架还通过跨链智能合约实现激励以保证设备的可靠性；文献[57]为了解决物联网环境下低性能设备带来的效率低下问题，提出了一种基于区块链的动态缩放因子异步 FL 框架。在此架构中，各节点基于动态缩放因子确定本地模型与全局模型的权重，再进行聚合并上传至区块链，通过动态缩放因子调整权重，降低滞后设备带来的消极影响，

提高了FL框架的收敛速度和训练精度。同时,采用了基于委员会的共识算法,保证了区块链网络的效率和安全性。此外,文献[58]提出一种区块链激励的、无须聚合器的FL框架(blockchain based aggregator free federated learning environment, BAFFLE)。该框架通过对智能合约编写成功取代了中央服务器,通过模型划分以及序列化机制,支持独立和并行的模型更新,从而提高了计算效率,并在保证精度的情况下降低了开销。文献[59]通过设计新的共识机制确保高效经济地使用区块链进行FL,通过预定义的方式设定参与节点数,并在每一轮都选择一个节点作为聚合节点,由其发布并聚合全局模型供其他节点进行训练,同时不断检查其他节点的本地链,当收到足够数量本地模型后生成全局模型并上传,同时,将区块链产生的分叉进行线性附加生成,缩短了共识时间。但是预定义的形式在一定程度上限制了通用性,同时仍存在恶意节点的威胁。

在实际部署过程中,首先必须考虑工作效率,本文对这方面的工作进行了总结(见表5),目前的工作主要通过提高模型计算效率和模型收敛速度提高整体的系统效率,即通过简化区块链的工作缩短时间成本,通过异步聚合的方式提高训练效率。然而,大部分工作在提高系统效率的同时面临着系统通信、计算开销高,安全性和隐私性无法得到有力保障的问题,如何平衡三者之间的关系仍需要进一步研究。目前,区块链赋能FL的效率方法已经广泛应用于边缘计算[55-56]、物联网[57]、数据分析[59]等领域,在提高FL安全性的同时实现了工作效率的提升,降低了时延及能耗。

表5 区块链赋能FL效率方法

Table 5 Efficiency methods of blockchain enabled FL

文献	区块链/共识	时延/ms	时间成本/s	主要贡献	不足
[55]	Ethereum/联盟链 PBFT			模型收敛速度快 计算效率高	未经过实际验证 只支持单个请求者的交易市场
[56]	/BFT型		3.05	学习精度高 时延低,性能稳定 保证设备的可靠性	计算开销高 网络开销高 未考虑设备的移动性和网络攻击
[57]	/基于委员会的共识算法	2.97		模型收敛速度快 模型训练准确性高	动态因子在简单数据集和模型上无明显优势 未考虑数据集大小不均及设备数量差异的影响
[58]	Ethereum/PoA			计算效率高 开销低 模型收敛速度快、质量高	不适用于大型场景 模型收敛速度较慢
[59]		19.00		共识时间短 模型精度高	通用性差 容易遭受搭便车攻击 容错性低

5 挑战与展望

下面,基于目前的研究进展从安全、效率、激励以及开销4个方面讨论区块链赋能FL面临的挑战,并进一步展望相关的解决方案。

1) FL中的恶意以及低效率节点。恶意参与者的存在会对FL系统造成安全和隐私方面的威胁,而在通过同步方式进行模型更新的FL中,需要所有本地模型更新后再聚合全局模型。因此,低效率参与者的存在会降低模型的收敛速度,延长训练时间。

对于FL节点的问题,可以设计节点认证方案,在节点加入FL训练任务之前,对这些设备进行注册并生成唯一的身份标识,从而有利于在之后的训练过程中,从设备训练时延、模型传输时延和模型准确率等方面对设备进行审核,保留符合要求的节点,避免恶意节点及懒惰节点的存在。

2) 效率。在FL过程中,由于参与者与服务器之间直接进行通信,当参与者数量过多时,会出现通信瓶颈。从区块链角度看,共识过程同样造成了通

信延迟以及更新偏差，降低了 FL 的性能。

FL 可以通过压缩模型上传的方法减少每个模型传输过程中的数据量，然而这种方法有可能造成模型上传精度损失，因此，可以考虑采用适当的量化数据级别来解决。同时，可以综合考虑资源、网络、计算等方面对算法进行优化，从而提高模型训练的效率。从区块链角度则需要进一步考虑交易和成块相关的加密解密，以及认证和共识过程在不同场景下的不同需求，对其进一步细化，选取合适的方法有利于提升整体效率。

3）激励。进行模型训练往往需要消耗巨大的计算资源和存储资源，如果没有足够的激励，很难令节点主动加入模型训练。此外，由于参与者自身存在的计算能力差异，计算能力强、资源丰富的参与者更容易处于主导地位，从而获得更多的激励。因而，如何实现激励公平仍然面临挑战。

对于公平激励的问题，由于在区块链赋能的 FL 中各参与训练的节点自身的计算能力、资源以及数据集质量存在差异，可以建立个性化的激励机制，采取合理的评估方法，综合参与者的情况对其做出的贡献进行评估。例如，对于给模型训练任务做出贡献的参与者，综合其自身情况和训练的模型评估其做出的贡献，基于此得出贡献比例并进行激励，从而鼓励更多的设备参与训练。

4）开销。在 FL 中虽然无须对原始数据进行传输，但是在模型比较复杂的情况下需要进行成百上千次的训练，这对于 FL 参与者的通信带宽有较高的要求。在区块链网络中，节点所需存储的数据量越大，运行区块链网络需要的存储成本也越高。

在 FL 方面可以通过梯度压缩或者梯度稀疏化等策略减少通信开销，但是这 2 种方式对于模型的精度或收敛速度有较明显的影响，因此，需要设计更加合理的通信压缩方案。在区块链的角度则可以通过设计轻量级的共识算法、降低节点同步数据量等方法降低通信和计算开销。

参考文献：

[1] CHEN Y Q, QIN X, WANG J D, et al. FedHealth: a federated transfer learning framework for wearable healthcare [J]. IEEE Intelligent Systems, 2020, 35(4): 83-93.

[2] LONG G D, TAN Y, JIANG J, et al. Federated learning for open banking [M] // Federated Learning. Cham: Springer, 2020: 240-254.

[3] XU J, GLICKSBERG B S, SU C, et al. Federated learning for healthcare informatics [J]. Journal of Healthcare Informatics Research, 2021, 5(1): 1-19.

[4] ZHENG Z H, ZHOU Y Z, SUN Y L, et al. Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges [J]. Connection Science, 2022, 34(1): 1-28.

[5] SARWATE A D, CHAUDHURI K. Signal processing and machine learning with differential privacy algorithms and challenges for continuous data[J]. IEEE Signal Processing Magazine, 2013, 30(5): 86-94.

[6] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data [EB/OL]. [2023-05-31]. https://arxiv.org/abs/1602.05629.

[7] TRAN N H, BAO W, ZOMAYA A, et al. Federated learning over wireless networks: optimization model design and analysis [C] // IEEE Conference on Computer Communications. Piscataway, NJ: IEEE, 2019: 1387-1395.

[8] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems, 2020, 2: 429-450.

[9] WANG H Y, YUROCHKIN M, SUN Y K, et al. Federated learning with matched averaging [EB/OL]. [2023-05-31]. https://arxiv.org/abs/2002.06440.

[10] 孙恩昌，张卉，何若兰，等. 基于联邦学习的移动通信资源管理：方法、进展与展望[J]. 北京工业大学学报，2022，48(7)：783-793.
SUN E C, ZHANG H, HE R L, et al. Mobile communication resource management based on federated learning: methods, progress and prospect[J]. Journal of Beijing University of Technology, 2022, 48(7): 783-793. (in Chinese)

[11] PAN S J, YANG Q. A survey on transfer learning [J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 22(10): 1345-1359.

[12] FENG L, ZHAO Y Q, GUO S Y, et al. BAFL: a blockchain-based asynchronous federated learning framework[J]. IEEE Transactions on Computers, 2022, 71(5): 1092-1103.

[13] LI Y Z, CHEN C, LIU N, et al. A blockchain-based decentralized federated learning framework with committee consensus[J]. IEEE Network, 2021, 35(1): 234-241.

[14] SHOKRI R, STRONATI M, SONG C Z, et al. Membership inference attacks against machine learning models[C] // 2017 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2017: 3-18.

[15] CHEN X H, JI J L, LUO C Q, et al. When machine learning meets blockchain: a decentralized, privacy-preserving and secure design [C] // 2018 IEEE International Conference on Big Data. Piscataway, NJ:

IEEE, 2018: 1178-1187.
[16] LI Z H, YU H F, ZHOU T Y, et al. Byzantine resistant secure blockchained federated learning at the edge[J]. IEEE Network, 2021, 35(4): 295-301.
[17] BERGER C, PENZENSTADLER B, DRÖGEHORN O. On using blockchains for safety-critical systems [C] // Proceedings of the 4th International Workshop on Software Engineering for Smart Cyber-Physical Systems. New York: ACM, 2018: 30-36.
[18] ZHANG X, QIN R, YUAN Y, et al. An analysis of blockchain-based bitcoin mining difficulty: techniques and principles[C]//2018 Chinese Automation Congress. Piscataway, NJ: IEEE, 2018: 1184-1189.
[19] NGUYEN D C, PATHIRANA P N, DING M, et al. Blockchain for 5G and beyond networks: a state of the art survey [J]. Journal of Network and Computer Applications, 2020, 166: 102693.
[20] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//2017 IEEE International Congress on Big Data. Piscataway, NJ: IEEE, 2017: 557- 564.
[21] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm [C]//Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference. Berkeley, CA: USENIX Association, 2014: 305-320.
[22] WU S H, DU J. Electronic medical record security sharing model based on blockchain[C]//Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. New York: ACM, 2019: 13-17.
[23] YANG R Z, YU F R, SI P B, et al. Integrated blockchain and edge computing systems: a survey, some research issues and challenges [J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1508-1532.
[24] NGUYEN D C, PATHIRANA P N, DING M, et al. BEdgeHealth: a decentralized architecture for edge- based IoMT networks using blockchain[J]. IEEE Internet of Things Journal, 2021, 8(14): 11743-11757.
[25] MILLER A, JUELS A, SHI E, et al. Permacoin: repurposing Bitcoin work for data preservation[C]//2014 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2014: 475-490.
[26] KING S, NADAL S. PPCoin: peer-to-peer crypto-currency with proof-of-stake[EB/OL]. [2023-05-31]. https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf.
[27] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]//Proceedings of the Third Symposium on Operating Systems Design and Implementation. Berkeley, CA: USENIX Association, 1999: 173-186.
[28] KHAN S N, LOUKIL F, GHEDIRA-GUEGAN C, et al. Blockchain smart contracts: applications, challenges, and future trends [J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2901-2925.
[29] LU Y L, HUANG X H, ZHANG K, et al. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks [J]. IEEE Transactions on Industrial Informatics, 2021, 17(7): 5098-5107.
[30] MAJEED U, KHAN L U, YOUSAFZAI A, et al. ST-BFL: a structured transparency empowered cross-silo federated learning on the blockchain framework [J]. IEEE Access, 2021, 9: 155634-155650.
[31] KORKMAZ C, KOCAS H E, UYSAL A, et al. Chain FL: decentralized federated machine learning via blockchain[C]//2020 Second International Conference on Blockchain Computing and Applications. Piscataway, NJ: IEEE, 2020: 140-146.
[32] MA C, LI J, SHI L, et al. When federated learning meets blockchain: a new distributed learning paradigm [J]. IEEE Computational Intelligence Magazine, 2022, 17(3): 26-33.
[33] KIM H, PARK J, BENNIS M, et al. Blockchained on-device federated learning [J]. IEEE Communications Letters, 2020, 24(6): 1279-1283.
[34] UNAL D, HAMMOUDEH M, KHAN M A, et al. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of things[J]. Computers & Security, 2021, 109: 102393.
[35] LIU Y, PENG J L, KANG J W, et al. A secure federated learning framework for 5G networks[J]. IEEE Wireless Communications, 2020, 27(4): 24-31.
[36] QIN Z, DENG S G, YAN X Q, et al. Secure and efficient decentralized federated learning with data representation protection [EB/OL]. [2023-05-31]. https://arxiv.org/abs/2205.10568.
[37] ZHANG P, LIU G, CHEN Z Y, et al. A study of a federated learning framework based on the interstellar file system and blockchain: private blockchain federated learning [C] // 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications. Piscataway, NJ: IEEE, 2022: 267-273.
[38] FIRDAUS M, LARASATI H T, RHEE K H. A secure federated learning framework using blockchain and differential privacy [C] // 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing

(CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud. Piscataway, NJ: IEEE, 2022: 18-23.

[39] LI A J, CHANG X, MA J X, et al. VTFL: a blockchain based vehicular trustworthy federated learning framework [C] // 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference. Piscataway, NJ: IEEE, 2023: 1002-1006.

[40] FAN M C, YU H F, SUN G. Privacy-preserving aggregation scheme for blockchained federated learning in IoT [C] // 2021 International Conference on UK-China Emerging Technologies. Piscataway, NJ: IEEE, 2021: 129-132.

[41] CHEN B W, ZENG H H, XIANG T, et al. ESB-FL: efficient and secure blockchain-based federated learning with fair payment [J/OL]. IEEE Transactions on Big Data [2023-05-31]. https: // ieeexplore. ieee. org/document/9780227.

[42] TANG X Y, ZHU L H, SHEN M, et al. Secure and trusted collaborative learning based on blockchain for artificial intelligence of things [J]. IEEE Wireless Communications, 2022, 29(3): 14-22.

[43] ZHOU Z H, GUO C X, ZHANG X S, et al. A blockchain-based data sharing marketplace with a federated learning use case[C]//2023 IEEE International Conference on Blockchain and Cryptocurrency. Piscataway, NJ: IEEE, 2023: 1041-1044.

[44] SENGUPTA B, SENGUPTA S, NANDI S, et al. Blockchain and federated-learning empowered secure and trustworthy vehicular traffic[C]//2022 IEEE/ACM 15th International Conference on Utility and Cloud Computing. Piscataway, NJ: IEEE, 2022: 346-351.

[45] CHEN X Y, WANG T T, ZHANG S L. The design of reputation system for blockchain-based federated learning [C] // 2021 International Conference on Artificial Intelligence and Blockchain Technology. Piscataway, NJ: IEEE, 2021: 114-120.

[46] MOUDOUD H, CHERKAOUI S, KHOUKHI L. Towards a secure and reliable federated learning using blockchain [C]//2021 IEEE Global Communications Conference. Piscataway, NJ: IEEE, 2021: 1-6.

[47] DE BRITO GONÇALVES J P, DA SILVA VILLAÇA R. A blockchained incentive architecture for federated learning[C]//2022 IEEE International Conference on Blockchain. Piscataway, NJ: IEEE, 2022: 482-487.

[48] TOYODA K, ZHAO J, ZHANG A N S, et al. Blockchain-enabled federated learning with mechanism design[J]. IEEE Access, 2022, 8: 219744-219756.

[49] XU Y J, LU Z H, GAI K K, et al. BESIFL: blockchain-empowered secure and incentive federated learning paradigm in IoT[J]. IEEE Internet of Things Journal, 2023, 10(8): 6561-6573.

[50] CHEN Y R, ZHANG Y Y, WANG S W, et al. DIM-DS: dynamic incentive model for data sharing in federated learning based on smart contracts and evolutionary game theory [J]. IEEE Internet of Things Journal, 2022, 9(23): 24572-24584.

[51] BEHERA M R, UPADHYAY S, SHETTY S. Federated learning using smart contracts on blockchains, based on reward driven approach [EB/OL]. [2023-05-31]. https: // arxiv. org/abs/2107. 10243.

[52] BATOOLZ, ZHANG K W, TOEWS M. FL-MAB: client selection and monetization for blockchain-based federated learning[C] // Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing. New York: ACM, 2022: 299-307.

[53] CHEN Y B, LIN F L, CHEN Z Y, et al. Blockchain-based federated learning with contribution-weighted aggregation for medical data modeling[C] // 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems. Piscataway, NJ: IEEE, 2022: 606-612.

[54] WANG X F, ZHAO Y F, QIU C, et al. InFEDge: a blockchain-based incentive mechanism in hierarchical federated learning for end-edge-cloud communications [J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3325-3342.

[55] FAN S Z, ZHANG H B, ZENG Y C, et al. Hybrid blockchain-based resource trading system for federated learning in edge computing [J]. IEEE Internet of Things Journal, 2021, 8(4): 2252-2264.

[56] FENG L, YANG Z X, GUO S Y, et al. Two-layered blockchain architecture for federated learning over the mobile edge network[J]. IEEE Network, 2022, 36(1): 45-51.

[57] XU C H, QU Y Y, EKLUND P W, et al. BAFL: an efficient blockchain-based asynchronous federated learning framework [C] // 2021 IEEE Symposium on Computers and Communications. Piscataway, NJ: IEEE, 2021: 1-6.

[58] RAMANAN P, NAKAYAMA K. BAFFLE: blockchain based aggregator free federated learning [C]//2020 IEEE International Conference on Blockchain. Piscataway, NJ: IEEE, 2020: 72-81.

[59] KALITA K P, BORO D, BHATTACHARYYA D K. An efficient consensus algorithm for blockchain-based federated learning[C]//2023 International Conference on Intelligent Systems, Advanced Computing and Communication. Piscataway, NJ: IEEE, 2023: 1-7.

(责任编辑　梁　洁)